Mitigasi Serangan DoS Pada Jaringan *Software Defined Network*

TUGAS AKHIR

Diajukan Untuk Memenuhi
Persyaratan Guna Meraih Gelar Sarjana Strata 1
Teknik Informatika Universitas Muhammadiyah Malang

Oleh:

WINDI WIDIASTUTI

201410370311239

JURUSAN TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH MALANG

2018

LEMBAR PENGESAHAN

Mitigasi Serangan DoS Pada Jaringan *Software Defined Network*

TUGAS AKHIR

Diajukan Untuk Memenuhi
Persyaratan Guna Meraih Gelar Sarjana Strata 1
Teknik Informatika Universitas Muhammadiyah Malang

Disusun oleh:

WINDI WIDIASTUTI
201410370311239

Tugas Akhir ini telah diuji dan dinyatakan lulus melalui sidang majelis penguji pada tanggal 11 Januari 2019

Menyetujui,

Dosen Penguji I	Dosen Penguji II
Denar Regata Akbi, M.Kom	**Diah Risqiwati, S.T., M.T**
NIP. 108.1612.0591	**NIP. 108.1410.0545**

Mengetahui,
Ketua Jurusan Teknik Informatika

Gita Indah Marthasari, ST., M.Kom
NIP. 108.0611.0442

LEMBAR PERNYATAAN

Yang bertanda tangan di bawah ini:

Nama	: **Windi Widiastuti**
Tempat, Tanggal Lahir	: **Malang, 25 Juni 1996**
NIM	: **201410370311239**
Fakultas / Jurusan	: **Teknik / Teknik Informatika**

Dengan ini saya menyatakan bahwa Tugas Akhir dengan judul **"*Mitigasi Serangan DoS Pada Jaringan Software Defined Network*"** beserta seluruh isinya adalah karya saya sendiri dan bukan merupakan karya tulis orang lain, baik sebagian maupun keseluruhan, kecuali dalam bentuk kutipan yang telah disebutkan sumbernya.

Demikian surat pernyataan ini saya buat dengan sebenar-benarnya. Apabila kemudian ditemukan adanya pelanggaran terhadap etika keilmuan dalam karya saya ini atau ada klaim dari pihak lain terhadap keaslian karya saya ini maka saya siap menanggung segala bentuk resiko / sanksi yang berlaku.

Malang, 3 Januari 2019

Yang Membuat Pernyataan

Windi Widiastuti

Mengetahui,

Dosen Pembimbing I	Dosen Pembimbing II
Syaifuddin S.Kom., M.Kom	**Fauzi Dwi S S, S.T., M.Comp.Sc**
NIP. 108.1612.0590	**NIP. 180.3070.61992**

LEMBAR PERSETUJUAN

Mitigasi Serangan DoS Pada Jaringan *Software Defined Network*

TUGAS AKHIR

Oleh :
Windi Widiastuti
201410370311239

Telah Direkomendasikan Untuk Diajukan Sebagai Judul Tugas Akhir Di Teknik Informatika Universitas Muhammadiyah Malang

Menyetujui,

Dosen Pembimbing I	Dosen Pembimbing II
Syaifuddin S.Kom., M.Kom	**Fauzi Dwi S S, S.T., M.Comp.Sc**
NIP. 108.1612.0590	**NIP. 180.3070.61992**

KATA PENGANTAR

بِسْمِ ٱللَّهِ ٱلرَّحْمَٰنِ ٱلرَّحِيمِ

Alhamdulillah, puji syukur atas kehadirat Allah SWT atas segala nikmat, rahmat dan hidayah-Nya yang telah diberikan kepada penulis, tak lupa solawat dan salam semoga terlimpahkan kepada junjungan besar Nabi Muhammad SAW. Sehingga penulis dapat menyelesaikan Tugas Akhir yang berjudul:

"*Mitigasi Serangan Dos Pada Jaringan Software Defined Network*"

Tujuan dari penyusunan Tugas Akhir ini adalah sebagai pengajuan untuk memenuhi persyaratan guna meraih gelar sarjana strata 1 Teknik Informatika Universitas Muhammadiyah Malang.

Penulis sangat menyadari bahwa dalam penelitian dan penulisan tugas akhir ini masih terdapat banyak keterbatasan dan kekurangan. Oleh sebab itu, penulis sangat mengharapkan saran yang dapat bermanfaat serta berguna untuk perkembangan ilmu pengetahuan.

Malang, 3 Januari 2019

Penulis

Windi Widiastuti

DAFTAR ISI

ABSTRAK i
ABSTRACT ii
LEMBAR PERSEMBAHAN iii
KATA PENGANTAR iv
DAFTAR ISI v
DAFTAR GAMBAR vii
DAFTAR TABEL ix
BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 3
1.3 Tujuan Penelitian 3
1.4 Batasan Masalah 3
1.5 Sistematika Penulisan 4
BAB II LANDASAN TEORI 5
2.1 Penelitian Terdahulu 5
2.2 Software Defined Network 6
2.3 Controller 7
2.3.1 Ryu 8
2.3.2 Learning Switch Controller 9
2.4 OpenFlow 9
2.4.1 *Reactive* & *Proactive* 10
2.5 OpenvSwitch 10
2.6 Denial of Services 10
2.6.1 Icmp *Flood* 11
2.7 Mininet 12
2.8 Scapy 12
2.9 Tcpreplay 13
2.10 Iperf 13
2.11 Wireshark 13
BAB III METODOLOGI PENELITIAN 15
3.1 Metode Penelitian 15
3.1.1 Identifikasi Masalah 15

3.1.2 Implementasi 16
3.1.3 Perancangan Topologi 17
3.1.3.1 Instalasi *Software* 17
3.1.3.2 Konfigurasi *Software* 18
3.1.4 Perancangan Sistem 19
3.1.4.1 Rancangan Serangan DoS 19
3.1.4.2 Rancangan Aturan Mitigasi 20
3.1.5 Skenario Pengujian 22
3.1.6 Pengujian 23
3.1.6.1 Non Rule Mitigasi 24
3.1.6.2 *Rule* Mitigasi 30
3.1.6.2.1 Identifikasi, Deteksi, dan Mitigasi 33
BAB IV HASIL DAN PEMBAHASAN 36
4.1 Hasil Pengujian 36
4.1.1 Pengukuran Rata-rata Jumlah *Packet In* dan *Packet Out* 36
4.1.2 Pengukuran Rata-rata Jumlah Nilai CPU 39
4.1.3 Pengukuran Nilai *Packet Loss* 40
4.1.4 Analisis *Flow Tabel* pada OVS 42
BAB V PENUTUP 44
5.1 Kesimpulan 44
5.2 Saran 44
DAFTAR LAMPIRAN 49

DAFTAR TABEL

Tabel 2. 1 Penelitian Terdahulu..... 5
Tabel 2. 2 Type Message ICMP..... 11
Tabel 3. 1 Kebutuhan Perangkat Keras..... 16
Tabel 3. 2 Kebutuhan Perangkat Lunak..... 16
Tabel 3. 3 Hasil Pengujian 1 untuk Rata-rata Jumlah Packet In dan Packet Out. 22
Tabel 3. 4 Hasil Pengujian 2 untuk Rata-rata Jumlah Nilai CPU..... 22
Tabel 3. 5 Hasil Pengujian 3 untuk Nilai Packet Loss dengan Bandwidth 10 Mb23
Tabel 3. 6 Hasil Pengujian 3 untuk Nilai Packet Loss dengan Bandwidth 50 Mb23
Tabel 3. 7 Kode Sumber Pembuatan Serangan DoS ICMP Flood..... 23
Tabel 3. 8 Kode Sumber Pengukuran nilai CPU perdetik..... 27
Tabel 3. 9 Kode Sumber Mengukur Rata-rata nilai CPU..... 28
Tabel 3. 10 Kode Sumber Inti Identifikasi, Deteksi dan Mitigasi..... 33
Tabel 3. 11 Tabel Pengaturan Priority pada Flow Rule..... 35
Tabel 4. 1 Hasil Rata-rata Jumlah Packet In dan Packet Out..... 36
Tabel 4. 2 Hasil Rata-rata Jumlah Nilai CPU pada Controller..... 39
Tabel 4. 3 Hasil Packet Loss pada Jaringan..... 40

DAFTAR GAMBAR

Gambar 2. 1 Arsitektur *Software Defined Network* 7
Gambar 3. 1 Tahapan Metodologi Penelitian 15
Gambar 3. 2 Perancangan Topologi *Single* 4 17
Gambar 3. 3 Konfigurasi Pembuatan Topologi *Single* 18
Gambar 3. 4 Konfigurasi untuk Menjalankan *Controller* Ryu 19
Gambar 3. 5 Konfigurasi Cek *Flow Table* 19
Gambar 3. 6 *Flowchart* Aturan Mitigasi 21
Gambar 3. 7 Konfigurasi Membuat Topologi *Single* 4 24
Gambar 3. 8 Konfigurasi Menjalankan Ryu *Controller* 24
Gambar 3. 9 Konfigurasi Menjalankan Serangan DoS ICMP *Flood* 25
Gambar 3. 10 *Capture* Serangan DoS ICMP dengan Wireshark 26
Gambar 3. 11 Filter *Packet In* 26
Gambar 3. 12 Filter *Packet Out* 26
Gambar 3. 13 Nomor PID dari *Controller ryu-manager* 27
Gambar 3. 14 Pengukuran Jumlah Nilai CPU per detik 27
Gambar 3. 15 Mengukur Rata-rata Jumlah Nilai CPU 28
Gambar 3. 16 Pengukuran Nilai *Packet Loss* 29
Gambar 3. 17 Konfigurasi Membuat Topologi Single 4 30
Gambar 3. 18 Konfigurasi Menjalankan Serangan DoS ICMP *Flood* 30
Gambar 3. 19 Konfigurasi Menjalankan Aturan Mitigasi 30
Gambar 3. 20 Capture Serangan DoS Menggunakan Wireshark 31
Gambar 3. 21 Filter *Packet In* 31
Gambar 3. 22 Filter *Packet Out* 31
Gambar 3. 23 Nomor PID *Controller* dari ryu-manager 32
Gambar 3. 24 Pengukuran Nilai CPU per detik pada *Controller* 32
Gambar 3. 25 Mengukur Rata-rata Nilai CPU pada *Controller* 32
Gambar 3. 26 Pengukuran Nilai *Packet Loss* 33
Gambar 3. 27 Hasil Proses Identifikasi, Deteksi dan Mitigasi 35
Gambar 4. 1 Rata-rata Jumlah *Packet In* 37
Gambar 4. 2 Rata-rata Jumlah *Packet Out* 38
Gambar 4. 3 Rata-rata Jumlah Nilai CPU pada *Controller* 39

Gambar 4. 4 *Packet Loss* pada Jaringan dengan Waktu 3 menit..... 41
Gambar 4. 5 *Packet Loss* pada Jaringan dengan Waktu 10 menit..... 41
Gambar 4. 6 *Flow Table Non Rule* Mitigasi..... 42
Gambar 4. 7 *Flow Table Rule* Mitigasi 43

DAFTAR LAMPIRAN

Lampiran 1 : Pengukuran Rata-rata Jumlah Packet In dan Packet Out 1000 pkt/s49
Lampiran 2 : Pengukuran Rata-rata Jumlah Packet In dan Packet Out3000 pkt/s50
Lampiran 3 : Pengukuran Rata-rata Jumlah Packet In dan Packet Out 5000 pkt/s51
Lampiran 4 : Pengukuran Rata-rata Jumlah Packet In dan Packet Out 20.000 pkt/s 52
Lampiran 5 : Pengukuran Rata-rata Jumlah Packet In dan Packet Out 1000 pkt/s 53
Lampiran 6 : Pengukuran Rata-rata Jumlah Packet In dan Packet Out 3000 pkt/s 54
Lampiran 7 : Pengukuran Rata-rata Jumlah Packet In dan Packet Out 5000 pkt/s 55
Lampiran 8 : Pengukuran Rata-rata Jumlah Packet In dan Packet Out 20.000 pkt/s 56
Lampiran 9 : Pengukuran Nilai CPU controller 1000 pkt/s 3 menit 57
Lampiran 10 : Pengukuran Nilai CPU controller 3000 pkt/s 3 menit 58
Lampiran 11 : Pengukuran Nilai CPU controller 5000 pkt/s 3 menit 59
Lampiran 12 : Pengukuran Nilai CPU controller 20.000 pkt/s 3 menit 60
Lampiran 13 : Pengukuran Nilai CPU controller 1000 pkt/s 3 menit 61
Lampiran 14 : Pengukuran Nilai CPU controller 3000 pkt/s 3 menit 62
Lampiran 15 : Pengukuran Nilai CPU controller 5000 pkt/s 3 menit 63
Lampiran 16 : Pengukuran Nilai CPU controller 20.000 pkt/s 3 menit 64
Lampiran 17 : Pengukuran Nilai Packet Loss 10.000 pkt/s 10 Menit 65
Lampiran 18 : Pengukuran Nilai Packet Loss 20.000 pkt/s 3 menit 66
Lampiran 19 : Pengukuran Nilai Packet Loss 10.000 pkt/s 10 menit 67
Lampiran 20 : Pengukuran Nilai Packet Loss 20.000 pkt/s 3 menit 68
Lampiran 21 : Pengukuran Nilai Packet Loss 10.000 pkt/s 10 menit 69
Lampiran 22 : Pengukuran Nilai Packet Loss 20.000 pkt/s 3 menit 70
Lampiran 23 : Pengukuran Nilai Packet Loss 10.000 pkt/s 10 menit 71
Lampiran 24 : Pengukuran Nilai Packet Loss 20.000 pkt/s 3 menit 72

DAFTAR PUSTAKA

[1] K. Kalkan, G. Gür, and F. Alagöz, "Defense Mechanisms Against DDoS Attacks in SDN Environment," vol. 55, no. 9, pp. 175–179, 2017.

[2] Z. Han, S. Member, X. Li, and K. Huang, "A Software Defined Network based Security Assessment Framework for CloudIoT," vol. XX, no. X, pp. 1–11, 2018.

[3] D. Prasetiawan, M. Abdurohman, and F. A. Yulianto, "Improving Distributed Denial Of Service (DDOS) Detection Using Entropy Method In Software Defined Network (SDN)," no. 01, 2017.

[4] H. Polat and O. Polat, "The Effects of DoS Attacks on ODL and POX SDN Controllers," pp. 554–558, 2017.

[5] Q. Yan and F. R. Yu, "Distributed Denial of Service Attacks in Software-Defined Networking with Cloud Computing," vol. 53, no. 4, pp. 52–59, 2015.

[6] P. Rengaraju, R. R. V, and C. Lung, "Detection and Prevention of DoS attacks in Software-Defined Cloud Networks," pp. 217–223, 2017.

[7] W. Navid, "Detection and Mitigation of Denial of Service (DoS) Attacks Using Performance Aware Software Defined Networking (SDN)," pp. 47–57, 2017.

[8] Y. E. Oktian, S. Lee, and H. Lee, "Mitigating Denial of Service (DoS) Attacks in OpenFlow Networks," pp. 325–330, 2014.

[9] S. Singh, "Prevention Mechanism for Infrastructure based Denial-of-Service attack over Software Defined Network," pp. 348–353, 2015.

[10] M. H. Hidayat, N. R. Rosyid, Y. Sekip, U. Iv, and Y. Indonesia, "Analisis Kinerja dan Karakteristik Arsitektur Software-Defined Network Berbasis OpenDaylight Controller," pp. 194–200, 2017.

[11] A. Parikh, "Software-Defined Networking (SDN) Definition," *The Linux Foundation*, 2018. [Online]. Available: https://www.opennetworking.org/sdn-definition/.

[12] A. P. Morreale and M. james Anderson, *Software Defined Networking: Design and Deployment*. CRC Press, 2015.

[13] P. M. Ombase, P. G. Scholar, and P. G. Scholar, “Survey on DoS Attack Challenges in Software Defined Networking,” vol. 173, no. 2, pp. 19–25, 2017.

[14] K. Anam, R. Adrian, J. Yacaranda, S. Unit, and Y. Indonesia, “Analisis Performa Jaringan Software Defined Network Berdasarkan Penggunaan Cost Pada Protokol Ruting Open Shortest Path First .,” pp. 1–8, 2017.

[15] Admin, “Build SDN Agilely,” *Ryu SDN Framework Community*, 2017. [Online]. Available: https://osrg.github.io/ryu/. [Accessed: 12-Dec-2018].

[16] L. Scott, “Understanding the Ryu API (Dissecting Simple Switch),” *Inside Openflow*, 2017. [Online]. Available: https://inside-openflow.com/2016/07/21/ryu-api-dissecting-simple-switch/. [Accessed: 15-Dec-2018].

[17] J. Casey and A. Sutton, “Openflow,” *Flowgrammable*, 2018. [Online]. Available: http://flowgrammable.org/sdn/openflow/#tab_switch. [Accessed: 15-Dec-2018].

[18] P. Zhang, H. Wang, C. Hu, and C. Lin, “On Denial of Service Attacks in Software Defined Networks,” no. December, pp. 28–33, 2016.

[19] Admin, “Production Quality, Multilayer Open Virtual Switch,” *Linux Foundation*, 2016. [Online]. Available: https://www.openvswitch.org/.

[20] P. Bera, A. Saha, and S. K. Setua, “Denial Of Service Atack in Software Defined NEtwork,” pp. 497–501, 2016.

[21] Admin, “Ping Flood (ICMP Flood),” *Imperva Incapsula*, 2018. [Online]. Available: https://www.incapsula.com/ddos/attack-glossary/ping-icmp-flood.html. [Accessed: 15-Dec-2018].

[22] M. Team, “Mininet Overview,” 2018. [Online]. Available: http://mininet.org/overview/. [Accessed: 15-Dec-2018].

[23] P. Biondi, “Scapy,” 2018. [Online]. Available: https://scapy.net/. [Accessed: 15-Dec-2018].

[24] F. Klassen, “Tcpreplay - Pcap editing and replaying utilities,” 2016. [Online]. Available: https://tcpreplay.appneta.com/. [Accessed: 15-Dec-2018].

[25] C. Partsenidis, “What is iPerf, and how do iPerf commands work?,”

Techtarget, 2016. [Online]. Available: https://searchnetworking.techtarget.com/answer/What-is-iPerf-and-how-is-it-used. [Accessed: 15-Dec-2018].

[26] G. Combs, "What is Wireshark ?," *The Wireshark Foundation*. [Online]. Available: https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html. [Accessed: 15-Dec-2018].

[27] O. Salman, I. H. Elhajj, A. Kayssi, and A. Chehab, "SDN Controllers : A Comparative Study," no. 978, pp. 18–20, 2016.